Exemplo de Configuração de DNS Doctoring no ASA

Contents

Introdução

Este documento mostra como o DNS Doctoring é usado no Adaptive Security Appliance (ASA) para alterar os endereços IP incorporados nas respostas do Domain Name System (DNS) para que os clientes possam se conectar ao endereço IP correto dos servidores.

Pré-requisitos

Requisitos

O DNS Doctoring requer a configuração da Network Address Translation (NAT) no ASA, bem como a habilitação da inspeção de DNS.

Componentes Utilizados

As informações neste documento são baseadas no Adaptive Security Appliance.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

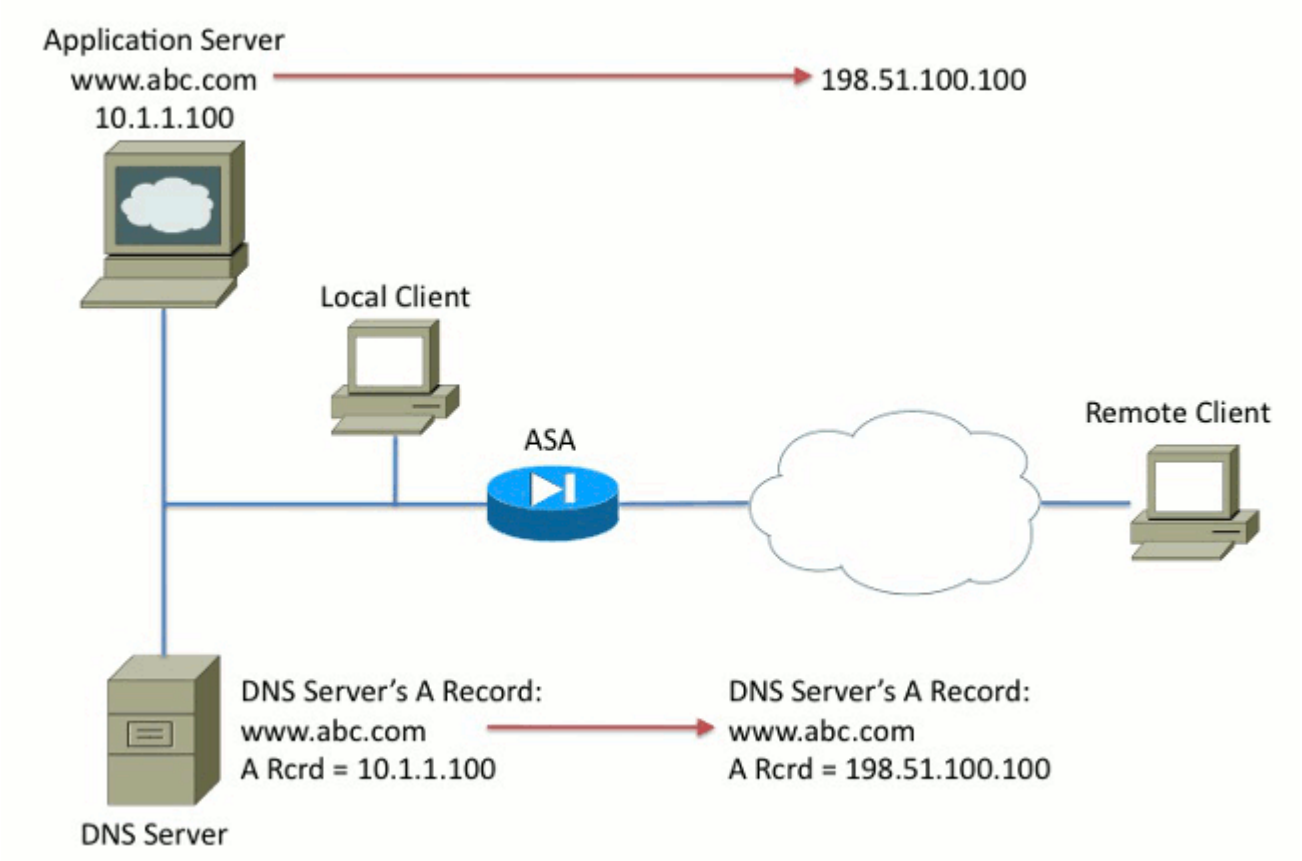
Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Exemplos de DNS Doctoring

Servidor DNS no interior do ASA

Figure 1



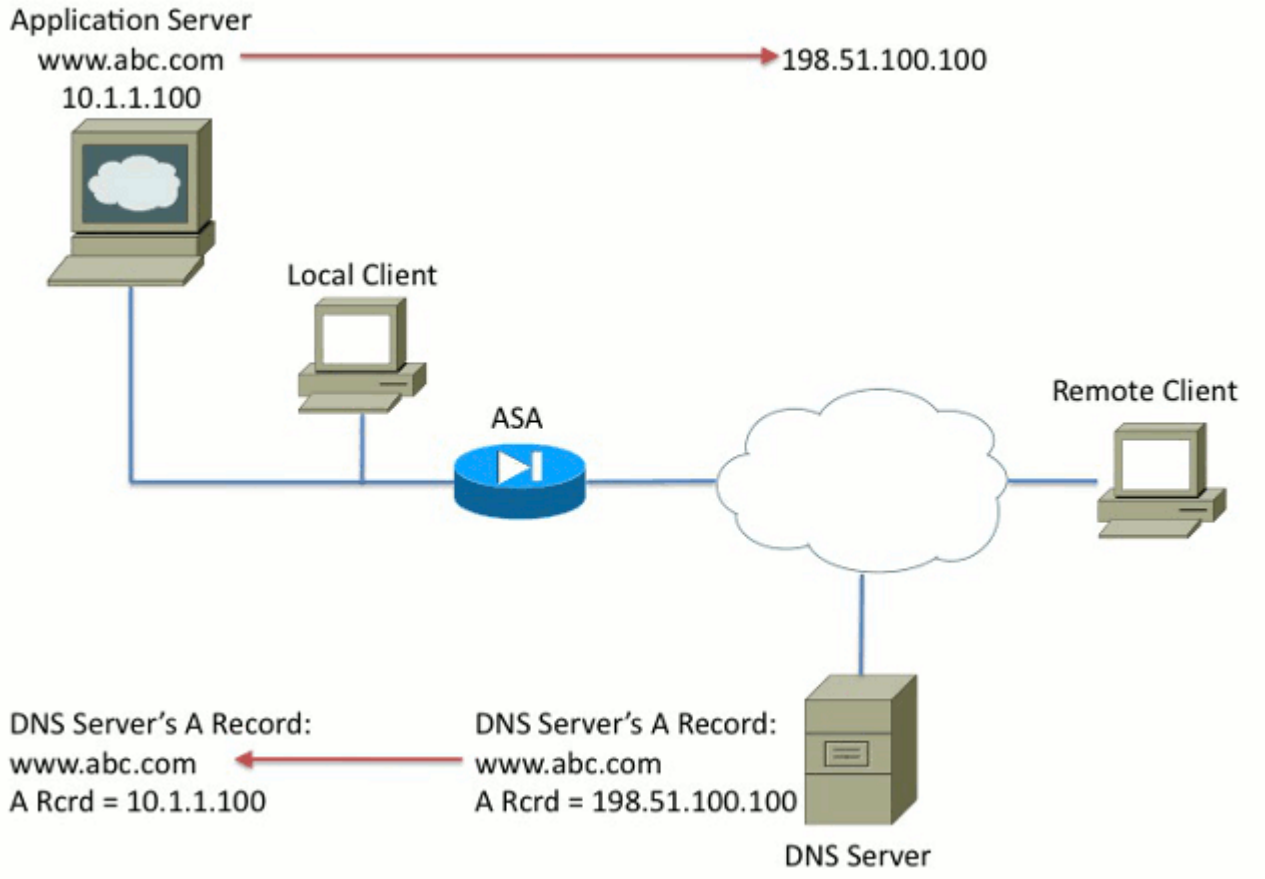

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

Na figura 1, o servidor DNS é controlado pelo administrador local. O servidor DNS deve distribuir um endereço IP privado, que é o endereço IP *real* atribuído ao servidor de aplicativos. Isso permite que o cliente local se conecte diretamente ao servidor de aplicativos.

Infelizmente, o cliente remoto não pode acessar o servidor de aplicativos com o endereço privado. Como resultado, o DNS Doctoring é configurado no ASA para alterar o endereço IP incorporado no pacote de resposta DNS. Isso garante que quando o cliente remoto faz uma solicitação DNS para www.abc.com, a resposta que eles obtêm é para o endereço convertido do servidor de aplicativos. Sem a palavra-chave DNS na instrução NAT, o cliente remoto tenta se conectar a 10.1.1.100, o que não funciona porque esse endereço não pode ser roteado na Internet.

Servidor DNS fora do ASA

Figure 2



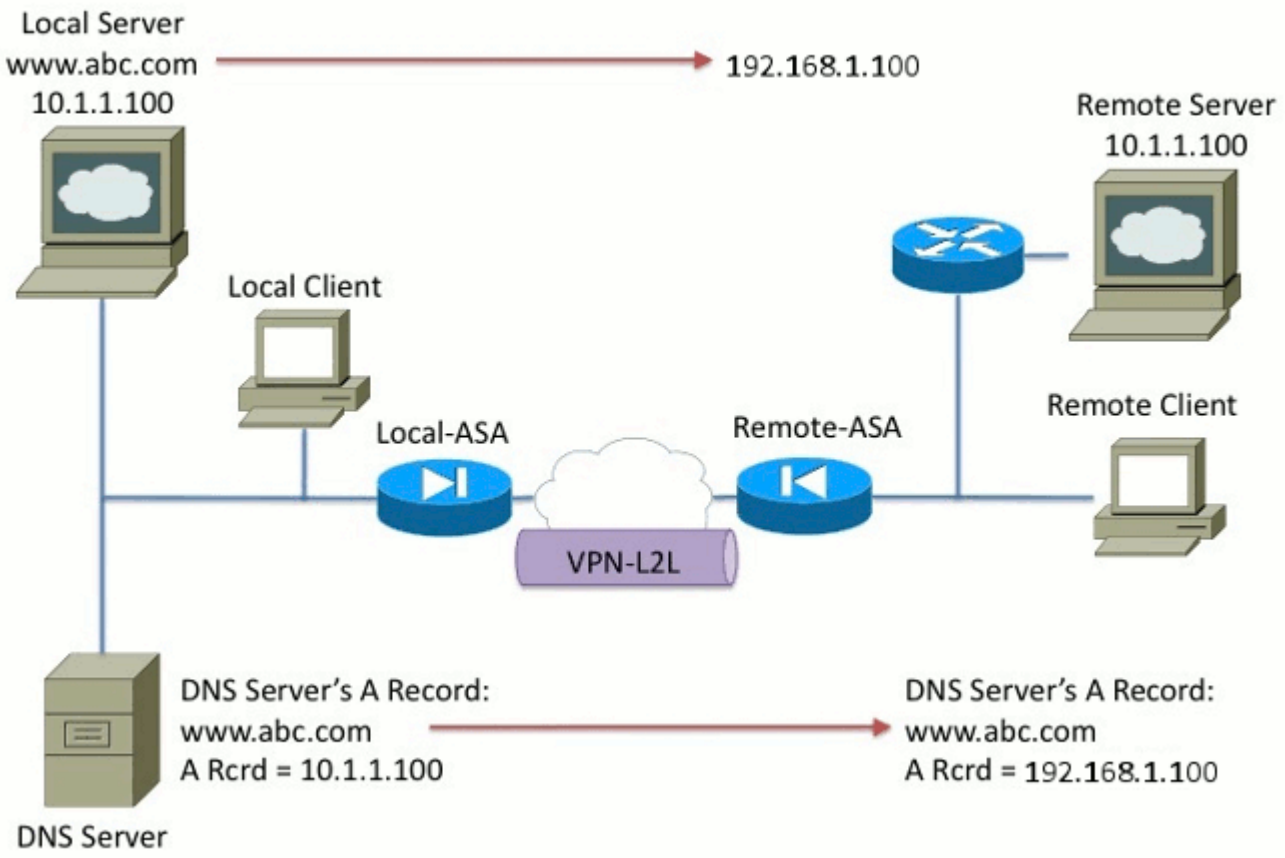

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

Na figura 2, o servidor DNS é controlado pelo ISP ou por um provedor de serviços similar. O servidor DNS deve distribuir o endereço IP público, ou seja, o endereço *IP* convertido do servidor de aplicativos. Isso permite que todos os usuários da Internet acessem o servidor de aplicativos pela Internet.

Infelizmente, o cliente local não pode acessar o servidor de aplicativos com o endereço público. Como resultado, o DNS Doctoring é configurado no ASA para alterar o endereço IP incorporado no pacote de resposta DNS. Isso garante que quando o cliente local faz uma solicitação DNS para www.abc.com, a resposta recebida seja o endereço real do servidor de aplicativos. Sem a palavra-chave DNS na instrução NAT, o cliente local tenta se conectar a 198.51.100.100. Isso não funciona porque esse pacote é enviado para o ASA, que descarta o pacote.

NAT VPN e DNS Doctoring

Figure 3



Considere uma situação em que haja redes que se sobrepõem. Nessa condição, o endereço 10.1.1.100 reside no lado remoto e no lado local. Como resultado, você precisa executar o NAT no servidor local para que o cliente remoto ainda possa acessá-lo com o endereço IP 192.1.1.100. Para que isso funcione corretamente, é necessário o DNS Doctoring.

O DNS Doctoring não pode ser executado nesta função. A palavra-chave DNS só pode ser adicionada ao final de um NAT de objeto ou NAT de origem. O NAT duas vezes não suporta a palavra-chave DNS. Há duas configurações possíveis e ambas falham.

Falha na configuração 1: se você configurar o resultado final, ele converterá 10.1.1.1 em 192.1.1.1, não apenas para o cliente remoto, mas para todos na Internet. Como 192.1.1.1 não é roteável pela Internet, ninguém na Internet pode acessar o servidor local.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
```

Falha na configuração 2: se você configurar a linha NAT de DNS Doctoring após a linha NAT necessária duas vezes, isso causará uma situação em que o DNS Doctoring nunca funciona. Como resultado, o cliente remoto tenta acessar www.abc.com com o endereço IP 10.1.1.100, que não funciona.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

Informações Relacionadas

- **Dispositivos de segurança adaptáveis Cisco ASA 5500 Series**
- **Cisco ASA 5500 Series Adaptive Security Appliances > Downloads de software**
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.